REMARKS

Reconsideration and allowance of the above-referenced application are respectfully requested. Claims 1, 3, 5, 8-11, 16, 22, 25, 27, 30, 34, 37, 39, 41, 44-47, 52, 58, 60, 62, 65-68 and 73 have been amended, and 1-78 are pending in the application.

The objection to the drawings regarding Figures 2-4 is acknowledged. Formal drawings will be submitted upon the indication of allowable subject matter.

The claims have been amended to ensure the extension ".wav" is within quotation marks.

Claims 1, 37, and 58 were rejected under 35 USC §112, second paragraph, in paragraph 4 of the Office Action: these claims have been amended to specify that the user interface session is to enable a user to send a message. Further, each of these claims specify that the message is encrypted into an encrypted message and that the encrypted message is output to a determined destination. Hence, it is believed the basis for the rejection in paragraph 4 has been overcome.

Claims 1, 8, 11, 22, 30, 37, 44, 47, 58, 65, and 68 were rejected under §112, second paragraph, in paragraph 5 of the Office Action: these claims have been amended to specify that the request is for providing a user interface session (or generation of the user interface session) by the device performing the recited operation of receiving the request. The claims have been amended to specify "providing", as opposed to"establishment of" as suggested by the Examiner, ensure consistency with the specification (e.g., at page 10, lines 19-23 of the specification). The claims having been amended to specify "generation of" ensure consistency with existing claim language (see, e.g., claim 22, line 8 "an application runtime environment configured for *generating the user interface session...*").

Hence, claims 1, 8, 11, 22, 30, 37, 44, 47, 58, 65, and 68 as amended specify that the user interface session is provided by (or generated by) the device receiving the request. As apparent from the specification, the broadest reasonable interpretation does not require maintaining a persistent connection between the device *sending* the request (e.g., client device) and the device *receiving* the request, but rather permits the session to encompass multiple requests (e.g., HTTP client requests) and responses (e.g., HTTP server responses) between the device *sending* the request (e.g., client device) and the device *receiving* the request (e.g., server) across non-

persistent connections (e.g., HTTP), based on a tracking of session state (e.g., the "brownie" described at page 9, lines 10-15 of the specification).

Hence, claims 1, 8, 11, 22, 30, 37, 44, 47, 58, 65, and 68 as amended comply with §112, second paragraph.

Claims 9, 45, and 66 have been amended to specify that a decryption result, having been received from the invoked decryption utility relative to the supplying of the decryption key and the stored message, is output independent of the encryption key matching the decryption key. As described in 7, lines 1-2 and page 15, line 23 to page 16, line 3 of the specification, the decryption result is output independent of whether the keys match in order to minimize involvement in the encryption and decryption operations, ensuring scalability. Hence, these claims specify that an evaluation of the decryption result for *valid* (i.e., recognizable) data is not necessary; further, providing the decryption result independent of a match enables the identified destination subscriber to receive feedback as to whether the decryption key matched the encryption key. Hence, it is believed claims 9, 45, and 66 as amended satisfy §112, second paragraph.

The rejection of claims 22 and 30 under §112, second paragraph in paragraph 7 of the Official Action is respectfully traversed. There is no suggestion in these claims that that the claimed "IP-based interface" is the same as the "user interface session". In fact, these claims specify: (1) an interface configured for receiving a request *for generation of a user interface session*; and (2) an IP-based interface *enabling retrieval of subscriber profile attributes ... from an IP-based subscriber profile directory*. The claimed "interface configured for receiving a request" reads on the web server interface 96 of Fig. 3, and the claimed "IP-based interface" reads on the libraries 82 of Fig. 3 (that include, for example, an Application Programming *Interface* (API) (see, e.g., page 13, lines 3-13 of the specification) that access subscriber profile attributes from the LDAP directory 88. For these and other reasons, the §112 rejection of claims 22 and 30 should be withdrawn.

The rejection of claims 8, 44, 65 under §112, second paragraph is traversed. It is notoriously well known that recital of "a" is not absolutely necessary for the initial recital of an

element (consider "retrieving *stored messages*" is equivalent to "retrieving *a plurality of stored messages*"): further, the recital of "stored messages" adequately establishes antecedent basis for subsequent recitals of "the stored messages", and eliminates the necessity of formalistic recitals such as "the plurality stored messages" or "the plurality of the stored messages". One skilled in the art would certainly be able to acertain the scope of the claims in their current form.

For these and other reasons, the §112, second paragraph rejections should be withdrawn.

Claims 1, 2, 7-15, 18, 20, 22, 23, 26-32, 35-38, 43-50, 54, 56, 58, 59, 62, 64-71, 73, 75, and 77 stand rejected under 35 USC 103 in view of U.S. Patent No. 6,584,564 to Olkin in view of U.S. Patent No. 6,661,877 to Lee. This rejection is respectfully traversed.

Each of the claims are directed to receipt of a key *from* a requesting device, as part of a user interface session, in order to cause at least one of encryption or decryption of a message. In particular, each of the independent claims 1, 11, 22, 30, 37, 47, 58, and 68 specify: (1) receiving from a requesting device a request for providing (i.e., generation of) a user interface session; (2) generating for the requesting device as part of the user interface session a prompt for the user of the requesting device to supply a key (e.g., an encryption key for sending a message, or a decryption key for retrieval of a message); (3) causing encryption or decryption of the message based on the key received from the requesting device as part of the user interface session.

As described in the specification (e.g., page 9, lines 20-25 and pages 14-15 with respect to Figs. 5A and 5B), the "user interface session" is composed of *multiple transactions* between the requesting device the application server in order to provide to the user the appearance of an interactive messaging application session. The Examiner is reminded that, the broadest reasonable interpretation cannot be inconsistent with the specification. Hence, "claims are not to be read in a vacuum, and limitations therein are to be interpreted in light of the specification in giving them their 'broadest reasonable interpretation.'" MPEP § 2111.01 at 2100-37 (Rev. 1, Feb. 2000) (quoting In re Marosi, 218 USPQ 289, 292 (Fed. Cir. 1983)(emphasis in original)).

Hence, each of the independent claims enable a user of the requesting device to send and/or receive encrypted messages, *regardless of whether any encryption utility is installed on*

the requesting device that is in use by the user. These and other features are neither disclosed nor suggested in the applied prior art.

As admitted in the Official Action, Olkin fails to teach that the disclosed e-mail system could be implemented in a unified communications system. Moreover, Olkin fails to disclose or suggest a centralized messaging system that provides a user interface session for a requesting device and generates prompts for the requesting device as part of the user interface session that permits a user of the requesting device to supply a key via the requesting device, as claimed.

Olkin describes a secure e-mail system requiring a sending computer 18 and a receiver computer 12 to include encryption software modules 26 (described with respect to Figure 3):

> With respect to the software required, each sending unit 18 and receiving unit 20 will need suitable e-mail type applications ***and suitable instances of the software modules 26***.
>
> (Col. 5, lines 62-65).

Hence, Olkin requires that the sending user (i.e., "sender") 12 send an *encrypted* secure e-mail 14. In particular, sender 12 uses a "Send Securely" command to request transmission of a secure e-mail 14; the sending computer 18 first contacts a security server 24 and provides the security server with various data items (e.g., sender ID, sender password, and receiver ID). *The security server* neither discloses nor suggests the claimed feature of generating a prompt for the requesting device for the user to supply an encryption key as specified in claims 1, 22, 37, or 58; rather, as illustrated in Fig. 3 of Olkin, the encryption resource 26 is implemented in the *sender 18* and the *receiver* 26.

Hence, the assertion in the Official Action that "Olkin discloses a first [and second] prompt" is misleading, because the prompts are generated by the encryption resource 26 within the sender 18, and not the security server 24. In each of the cited portions (col. 3, line 30 - col. 4, line 25, col. 6, lines 23-67, col. 11, lines 35-67, col. 12, lines 20-56, col. 14, lines 23-45), Olkin *relies* on the encryption resources 26 being implemented in the sender 18 and the receiver 20, and that the security server 24 sends the encryption key to the sender and receiver:

In a stage 34, rather than use a "Send" command the sender 12 instead uses a "Send Securely" command to request transmission of the secure e-mail 14. However, ***rather than transmit the unsecured e-mail message immediately to the e-mail server 22***, the sending unit 18 first contacts the security server 24 and provides it with various data items (the respective data items used in this stage and others are described presently). The security server 24 then authenticates the sender 12 and replies to the sending unit 18 with a unique message key and id for the present secure e-mail 14. The security server 24 also logs various data items for this transaction which may be used later. Using the message key, the sending unit 18 now encrypts the secure e-mail 14. ***The message body, encrypted or otherwise, is never sent to the security server 24.***

(Col. 6, lines 29-43).

In a stage 40 ***the secure e-mail 14 arrives in the inbox of each receiver 16***. When a receiver 16 opens the secure e-mail 14, using their receiving unit 20, ***the software module 26 for the receiving unit 20 detects that the secure e-mail 14 is encrypted***. Depending upon its configuration, ***the software module 26*** can then prompt the receiver 16 for a password or use one already known to it.

Finally, in a stage 42 the receiving unit 20 contacts the security server 24 and provides it with the message id and data for the receiver 16 (including their password). Assuming that the receiver 16 is an authorized recipient (as determined by the list of recipients in the original message), the security server 24 provides the message key to the receiving unit 20. With the message key ***the receiving unit 20 decrypts the secure e-mail 14*** and the receiver 16 is able to read it.

(Col. 8, lines 7-25).

Hence, Olkin ***explicitly teaches away from*** sending the unencrypted message from the requesting device to the unified communications system, as specified in claims 1, 22, 37, or 58. Moreover, Olkin ***explicitly teaches away from*** receiving the encryption key from the requesting device and causing the encryption based on the encryption key having been received from the requesting device as part of the user interface session (as specified in claims 1, 22, 37, or 58) by *sending* the encryption key ***from*** the server 22 ***to*** the sender 18.

Olkin also ***explicitly teaches away from*** generating for the requesting device as part of the user interface session a prompt for the messaging subscriber to supply a decryption key (as

specified in claims 11, 30, 47, or 68), based on teaching that the prompt and decryption operations being performed *exclusively* in the receiver 20. Olkin also ***explicitly teaches away from*** receiving the decryption key from the requesting device and causing the decryption based on the decryption key having been received from the requesting device as part of the user interface session (as specified in claims 11, 30, 47, or 68) by *sending* the encryption key ***from*** the server 22 ***to*** the receiver 20.

Finally, Olkin provides no disclosure whatsoever of any user interface session between the server 22 and the sender or receiver: the claims specify that prompts are generated and sent to the requesting device as part of the user interface session; in contrast, Olkin simply provides a reply (the message key) in response to the sender 18 or receiver 20 having *initiated* the request by sending the data elements for generation of the key. There is no user interface session involving multiple prompts from the system and multiple responses from the requesting device, as claimed.

In fact, Olkin ***explicitly teaches away from*** generating for the requesting device as part of the user interface session the prompts:

> If the password 102b of the sender 12 is incorrect ***the software module 26 can be instructed to prompt for the password 102b again***....
>
> (Col. 13, lines 35-37).

Hence, Olkin repeatedly states that the software module 26 within the sender 12 or the receiver 20 initiates the prompts, receives the key from the server, and encrypts the message to ensure the unencrypted message is never sent outside the sender 12 ("[t]he message body, encrypted or otherwise, is never sent to the security server 24." (Col. 6, lines 42-43)).

Hence, Olkin limits server operations to supplying the encryption key, and *never supplies the message body or the encryption/decryption key to the server.* Any assertion in the Official Action that the "password" described in Olkin is equivalent to the claimed encryption key or decryption key is an unreasonable interpretation of the claims and an unreasonable interpretation of Olkin.

A prior art reference must be considered in its entirety, i.e., as a whole, including portions that would lead away from the claimed invention. MPEP §2141.02, page 2100-127 (Rev. 2, May 2004) (citing W.L. Gore & Assoc. v. Garlock, Inc., 220 USPQ 303 (Fed. Cir. 1983), cert. denied, 469 U.S. 851 (1984)).

Consequently, the hypothetical combination of Olkin and Lee would neither disclose nor suggest the claimed feature of a unified communications system that: (1) generates a prompt for the requesting device, based on the user selecting encryption of the message, for the user to supply an key; (2) causing encryption or decryption of the message based on the key supplied by the user via the requesting device, as claimed.

Rather, the hypothetical combination would at most provide a unified messaging system having a security server that supplies the encryption key. Lee simply provides a unified message store: there is no disclosure or suggestion to perform the encryption/decryption operations outside the sender or receiver, especially since such a modification would violate the consistent teachings of Olkin, namely encrypting ***only at the sender terminal***, and decrypting ***only at the receiver terminal.*** The Examiner is reminded that the proposed modification cannot change the principle operation of a reference or render it unsatisfactory for its intended purpose. "If the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims prima facie obvious." MPEP § 2143.02, Rev. 2, May 2004 at p. 2100-132 (Citing In re Ratti, 270 F.2d 810, 123 USPQ 349 (CCPA 1959). "If the proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification." Id. (Citing In re Gordon, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984)).

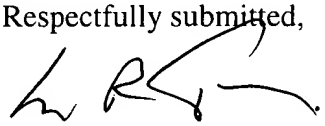
For these and other reasons, the rejection of claims 1, 2, 7-15, 18, 20, 22, 23, 26-32, 35-38, 43-50, 54, 56, 58, 59, 62, 64-71, 73, 75, and 77 should be withdrawn.

It is believed the remaining dependent claims are allowable in view of their dependency from the respective independent claims.

In view of the above, it is believed this application is and condition for allowance, and such a Notice is respectfully solicited.

To the extent necessary, Applicant petitions for an extension of time under 37 C.F.R. 1.136. Please charge any shortage in fees due in connection with the filing of this paper, including any missing or insufficient fees under 37 C.F.R. 1.17(a), to Deposit Account No. 50-1130, under Order No. 95-456, and please credit any excess fees to such deposit account.

Respectfully submitted,



Leon R. Turkevich
Registration No. 34,035

Customer No. 23164
Date: February 25, 2005